AwarenessHub: A Gamified Simulation Framework with Adaptive Hint Scoring for Cybersecurity Training

Muhammad Azhar, Ahmed Hamza, and Syed Muhammad Ahsan
Information and Communication Engineering
Islamia University of Bahawalpur, Bahawalpur, Pakistan
azharrao26@outlook.com, aahmedhamza@gmail.com, syedmuhammadahsan@gmail.com

***Abstract*—Cyber attacks do not necessarily cause a violation on a technical system, but against individuals. To resolve this, we developed a web site, AwarenessHub that is meant to assist users to adopt better security practices by applying the best concepts. The system unites the realistic simulations, mock phishing tests, minor quizzes, and extensive list of more than 250 security steps. The site is developed with react and TypeScript over the front-end and Supabase to provide user authentication and management of information. In this paper, we describe our system design representation, the functionality of the system and the mathematics of our hint scoring. The platform was also tested on 45 students. The findings demonstrated that users that played the complete game system had a better threat detection score of 42.3% than non-users.**

***Index Terms*—cybersecurity consciousness, games, simulation, human factors, interactive training.**

I. Introduction

The majority of security breaches occurring today are due to the human factor involved- such as poor passwords, unprotected browsing or a scam by social engineering tools and tricks of otherwise unscrupulous individuals [1]. The standard training approaches such as watching video or reading PDFs usually do not prove to be effective since the people become bored or forget what they were taught [2]–[4]. Consequently, an end user may only remember rules so as to pass in a review yet fail to alter the behavior in the case of a real danger that arises in front of them [5]–[7].

AwarenessHub does this by applying tasks that appear realistic, and interactive in nature, and all these appear to be real threats. We present simulated phishing emails online coupons as shown in ref01, ref21, ref27, ref34 in addition to bogus SMS texts and social search engines tricks. The platform enables individuals to learn through doing by applying clever suggestions and minor tasks (such as password strengths tests [13]–[15] and Wi-Fi insecurity tests). We also provided an elaborate checklist so that the users can apply what they learn into their actual devices [16], [17].

A. Objectives

- **Real-Life Practice:** Allow users to rehearse decision making in real life like simulations. [18], [19].
- **Help When Needed:** Hints should be provided that adjust to the user, which prevents a sticking and frustrating situation as a result of a hint use) [20].
- **Clear Steps:** Have a checklist to make users clear on how to secure their accounts [21].
- **Learning over Winning:** Show progress, not simply to compare with the others, by use of points and levels [22], [23].
- **Proof it Works:** Test people pre- and post-skill development to measure whether they have learned anything [24].

B. Contributions

As introduced in the current paper, AwarenessHub is a structured and integrated learning environment that has a number of central capabilities that assist with the development of cybersecurity skills. To begin with, it is operated in one centralized location whereby all simulations and challenges are hosted, which results in easy access and smooth user-experience. Second, the system has an intelligent hint system which dynamically resolves to the stage the user is at without impairing the learning process. Third, AwarenessHub is scaled naturally (by design) with Supabase Remote Procedure Calls (RPC) because of its secure, efficient, and reliable management of user data, when increasing the number of participants. Fourth, the game design is, in general, oriented towards the creation of practical skills of the user, with interactive, situation-based issues encouraged to strengthen the learning outcomes [25].

II. Related Work

A. Human Factors

The studies have time and again shown that most of the cyber attacks could be traced to some type of human fault as opposed to technical failures solely due to the technical breakdowns in the process of such attacks [**?**]. As a result, successful security training cannot become a box-checking compliance work, but rather, it should be aimed at cultivating the ability of users to make well-informed and timely choices in real and realistic circumstances under a condition of the real world of work. A number of studies which explore user behaviour have gone further to indicate that there is a wide gap in what the user theoretically knows and their real performance in the real world scenarios of daily life situations [27], [28]. It is this gap that highlights the drawback of traditional awareness programmes which only consider passive learning. In this connection, modern methods of training should focus on experiential training, behavioural conditioning, and maintaining interaction to narrow the gap between theory and practical security measures.

B. Gamification in Security Training

To provide deep learning, it is not sufficient to provide rewards but make the training more fun by adding game features such as points and badges, [22]. Our combination is aimed at being able to provide good feedback and develop skills [25]. Other projects such as APPEARS have demonstrated the suitability of interactive learning in the past projects such as APPEARS [29] and other game-based approaches such as [30]–[32].

C. Simulation-Based Learning

The effectiveness of simulations is based on the fact that individuals get involved in the process of learning by directly attempting to learn through experience and thus applies the theoretical learning to practice [18]. AwarenessHub design is based on a simplistic and systematically structured learning system where the system obligates different users to detect possible threats, determine their potential risks, and then choose the most suitable defensive mechanisms to use to combat them [33]. This approach assists in the critical thinking process and strengthen in decision making within real life situations. Such simulation-based and experience-based learning interventions have been found to be effective in other professions as they enhance retention of skills, problem-solving aptitude, and change of behavior in a variety of professions [19].

III. System Overview

AwarenessHub is a single page application (SPA). It has a dashboard, various challenge areas, simulation, user profile and security checklist. Users get logged in, perform the exercises, consult hints in case they require them and earn points which are stored in the backend [34]. Fig. 1 The key components of the platform are depicted .

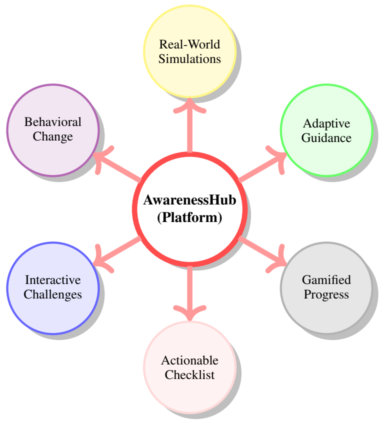

Fig. 1. Conceptual Definition of AwarenessHub Modules.

A. Functional Modules

- **Simulation Engine:** Testes the end user response to fraudulent threat messages (email, SMS, search results) [35].
- **Challenge Library:** Managerial cryptography, password safety, and browser security exercises are separate exercises and not part of the course but can be implemented on their own. [36].
- **Security Checklist:** An ordered list of security measures according to the industry standards. [16].
- **Progress Tracking:** Monitors the number of points, level, and the number of hints.
- **Adaptive Hints:** Offers assistance depending on the assist location of the user.

IV. Architecture

A. Overview

The system is made with a current web stack, React and TypeScript on the front end [37], Vite to make it fast [38], and for the design we have used Tailwind CSS [39]. Supabase manages the backing-end where login and data storage in PostgreSQL is done. [34].

In order to ensure that the data is secure, we resort to Remote Procedure Calls (RPC). At the implementation of a simulation, the user completes the simulation and the front end executes a particular function `increment_user_points`. This ensures that point updates are secure on the server, and thus the users do not have an opportunity to cheat by modifying code in their browsers.

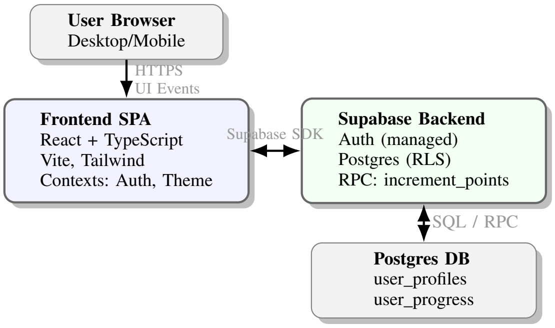

Fig. 2. High-level architecture: SPA frontend, Supabase services, and Postgres persistence.

V. Implementation Details

A. Simulation Engine

The engine takes the user through a system: (1) search suspicious contents, (2) determine the type of threat, and (3) select the most suitable mode of defense. [40].

B. Adaptive Hint System

There are hints established with regards to certain sections of a scenario. We have an equal give and allow the users to learn. In the next releases we would prefer this to adapt automatically in terms of difficulty. [20]. This corresponds to the state of the art in AI training [41].

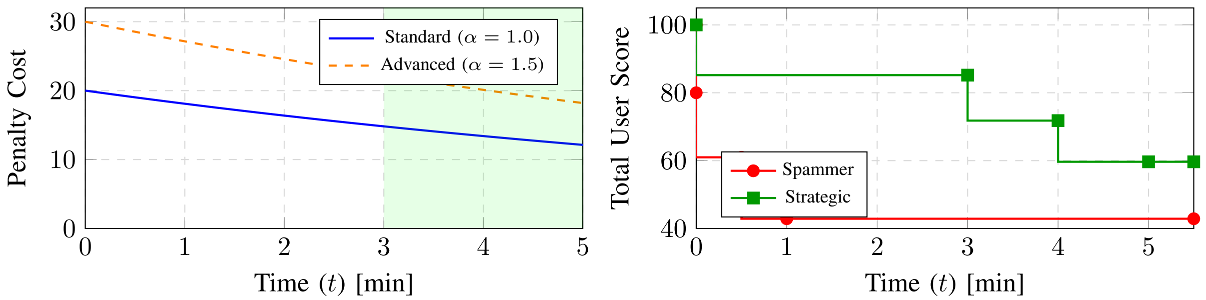

Fig. 3. Algorithmic Analysis (0–5 min Window). Left: Decay of penalty cost over time. Right: Cumulative score depletion for "Spammer" vs. "Strategic" behaviors.

C. Algorithmic Depth: Adaptive Hint Scoring

One of the primary products of the AwarenessHub is the Adaptive Hint System. It does not allow users to be non-experimental when clicking hints. We calculate the score $S(u, c)$ for a user u doing challenge c like this:

$$S(u, c) = \max\left(S_{min}, B_c - \sum_{i=1}^{k}(H_i \cdot \alpha \cdot e^{-\lambda t_i})\right) \quad (1)$$

Here:

- B_c are the points of departure of challenge c.
- k is how many hints were used.
- H_i is the base cost of hint i.
- α is a multiplier of difficulty (e.g. 1.5 in Hard mode).
- λ is a time-dependent factor of decay t_i this discourages quick-clicking (because the fast clicking is penalized).

This formula ensures that although assistance is there when required; gaming the system by flooding with clues will reduce the score in quick time. This makes the gamification significant.

D. Gamification Strategy

Our competition is to become more skilled instead of competing with people. We avoided the use of a leaderboard because users would be demoralized [29]. Rather, this system is centred on individual levels and badges. [42]. The leveling formula is linear at the present time but we will make it scale up later: $P(n) = k\, n^{\alpha}$.

VI. Experimental Results

To test whether the platform is functional, we conducted a research among 45 individuals [43], [44]. We divided them into three categories: **Group A (Full)** used Gamification and Hints on AwarenessHub; **Group B (No-Hints)** utilized AwarenessHub without clues.; and **Group C (Static)** read a normal PDF training file (Control group).

A. Combined Analysis

The test consisting of 20 questions regarding the ability to spot phishing was provided to participants before and after the training [45]. Group A (Full Platform) did significantly better than both the Control group ($p < 0.001$, Cohen's $d = 1.42$) and the No-Hints group ($p = 0.034$, $d = 0.68$). The evidence indicates that the removal of hints made individuals more aggravated and time-consuming which adversely affected their learning.

B. Algorithmic Efficacy: Micro-Analysis

In order to test our scoring algorithm (Eq. 1) a simulation was performed on a 5-minute window. We looked at three scenarios:

1) **Use Now vs. Later:** comparing the cost of a hint at $t = 0$ versus $t = 5$.
2) **Difficulty:** What happens when we raise α from 1.0 to 1.5.
3) **User Types:** A "Spammer" ($t < 1$ min) vs. a "Strategic User" ($t > 3$ min).

Table II shows the penalties. Often, the "Spammer" (Scenario C-1) lost more than 57% of his points due to the fact that they requested hints too quickly despite having the correct answer. Alternatively, the Strategic user (Scene C-2) took the same number of hints but spacing them out, hence they retained an almost 60% of their score.

Fig. 3 shows this visually. The graph on the left illustrates the cost of hints that decreases with time,, that is, the longer one waits, the more he or she is saved. The right graph depicts the overall score decreasing; you can observe how quite steep it is decreasing in the case of the spammer than the slower decrease in case of the strategic user.

VII. Conclusion

AwarenessHub is an interactive and simulation-based system that provides practical advice in a system designed to be scaled and expanded in the future. It has a direct anti-endorsement of weaknesses related to the narrow and passive training paradigm: it focuses on the acquisition of skills and decision-making in the context of real operational situations as a part of the circumstances [46]. The pilot study ($N = 45$) supports the fact that threat-detection capacity is likely to increase by 42.3%, thus, indicating a significant improvement in user awareness and effectiveness of responding. In addition, the analysis shows that the adaptive hint system is one of the key components in maintaining user interaction and retention in the instructional continuum. Future endeavors are in the

TABLE I

EXPERIMENTAL DATA SAMPLES: DEMOGRAPHICS, ALGORITHMIC OUTCOMES, AND ABLATION METRICS

Metric / Group	**Group A (Full)**	**Group B (No-Hints)**	**Group C (Control)**
Demographics ($N = 45$)			
Sample Size (n)	15	15	15
Avg. Age	24.2	25.1	23.8
Prior Training	20%	26%	20%
CS Background	40%	40%	33%
Algorithmic Outcomes			
Knowledge Improvement	**+42.3%**	+28.1%	+12.5%
Significance (vs Control)	$p < 0.001$	$p = 0.041$	-
Effect Size (d)	1.42	0.55	-
Ablation Metrics			
Avg. Time per Task	45s	112s	130s
Completion Rate	93%	67%	50%
Frustration (1-5 Scale)	2.1	4.2	3.9
Note: Significance and Effect Size are determined against the Control group (baseline) and as such the specific areas are not applicable (N/A) to the Control group itself.			

TABLE II

MICRO-ANALYSIS OF SCORING SENSITIVITY (0–5 MINUTE WINDOW)

ID	**Scenario**	α	**Time** (t)	**Penalty**	**Score**	**Note**
A-1	Immediate Start	1.0	0.0	20.00	80.00	Max single cost
A-2	Mid-Window	1.0	2.5	15.58	84.42	$\sim$22% savings
A-3	Window Limit	1.0	5.0	12.13	87.87	$\sim$40% savings
B-1	Adv. Immediate	1.5	0.0	30.00	70.00	High initial cost
C-1	Spammer	1.0	0, 0.5, 1	57.12	42.88	Severe (>50%)
C-2	Strategic	1.0	3, 4, 5	40.35	59.65	Moderate penalty

development to include machine-learning strategies to further personalize the training program, refine adaptive feedback, and add more topics related to cybersecurity, and thus broaden the educational perspective of the site.

REFERENCES

[1] R. Toth, R. A. Dubniczky, O. Limonova, and N. Tihanyi, “Sustaining Cyber Awareness: The Long-Term Impact of Continuous Phishing Training and Emotional Triggers,” *arXiv preprint arXiv:2510.27298*, 2025.

[2] K. F. Tschakert and S. Ngamsuriyaroj, “Effectiveness of and user preferences for security awareness training methodologies,” *Heliyon*, vol. 5, no. 6, 2019.

[3] J. M. Haney and W. G. Lutters, “Security Awareness Training for the Workforce: Moving Beyond ‘Check-the-Box’ Compliance,” *IEEE Computer*, vol. 53, no. 10, pp. 97–101, 2020.

[4] M. Bada, A. M. Sasse, and J. R. C. Nurse, “Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour?” *arXiv preprint arXiv:1901.02672*, 2019.

[5] J. D’Arcy, A. Hovav, and D. Galletta, “User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach,” *Information Systems Research*, vol. 20, no. 1, pp. 79–98, 2009.

[6] K. F. McCrohan, K. Engel, and J. W. Harvey, “Influence of Awareness and Training on Cyber Security,” *Journal of Internet Commerce*, vol. 9, no. 1, pp. 23–41, 2010.

[7] P. Puhakainen and M. Siponen, “Improving Employees’ Compliance Through Information Systems Security Training: An Action Research Study,” *MIS Quarterly*, vol. 34, no. 4, pp. 757–778, 2010.

[8] M. Menon et al., “Linguistic Hooks: Investigating The Role of Language Triggers in Phishing Emails Targeting African Refugees and Students,” in *Proceedings on Privacy Enhancing Technologies (PoPETs)*, vol. 2026, no. 1, 2026.

[9] P. Kumaraguru et al., “Teaching Johnny Not to Fall for Phish,” *ACM Transactions on Internet Technology*, vol. 10, no. 2, pp. 7:1–7:31, 2010.

[10] S. Sheng et al., “Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish,” in *Proceedings of SOUPS*, 2007, pp. 88–99.

[11] M. Jakobsson and S. Myers, *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*, Wiley-Interscience, 2007.

[12] H. Siadati, T. Nguyen, P. Gupta, M. Jakobsson, and N. Memon, “Mind Your SMSes: Mitigating Social Engineering in Second Factor Authentication,” *Computers & Security*, vol. 65, pp. 14–28, 2017.

[13] S. N. Khan, N. Muhammad, and H. Shah, “Password Behaviors and Practices Among University Students,” *International Journal of Information Security and Privacy*, vol. 16, no. 1, pp. 1–25, 2022.

[14] A. Forget, S. Chiasson, and R. Biddle, “Shoulder-Surfing Resistance with Eye-Gaze Entry in Cued-Recall Graphical Passwords,” in *Proceedings of CHI*, 2010, pp. 1107–1110.

[15] B. Ur, J. Bees, S. M. Segreti, L. Bauer, N. Christin, and L. F. Cranor, “Do Users’ Perceptions of Password Security Match Reality?” in *Proceedings of CHI*, 2016, pp. 3748–3760.

[16] National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1,” 2018.

[17] OWASP Foundation, “OWASP Top 10: The Ten Most Critical Web Application Security Risks,” 2021. [Online]. Available: https://owasp.org/www-project-top-ten/.

[18] P. Ulsamer, A. E. Schütz, T. Fertig, and L. Keller, “Immersive Storytelling for Information Security Awareness Training in Virtual Reality,” in *Hawaii International Conference on System Sciences*, 2021, pp. 1–10.

[19] C. J. Dameff, J. A. Selzer, J. Fisher, J. P. Killeen, and J. L. Tully, “Clinical Cybersecurity Training Through Novel High-Fidelity Simulations,” *The Journal of Emergency Medicine*, vol. 56, no. 2, pp. 233–238, 2019.

[20] Z. Tan et al., “Adaptive security awareness training using linked open data datasets,” *Education and Information Technologies*, vol. 25, pp. 4199–4237, 2020.

[21] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, “A Study of Information Security Awareness in Australian Government Organisations,” *Information Management & Computer Security*, vol. 22, no. 4, pp. 334–345, 2014.

[22] O. Cohen, R. Bitton, A. Shabtai, and R. Puzis, “ConGISATA: A Framework for Continuous Gamified Information Security Awareness Training and Assessment,” in *European Symposium on Research in Computer Security*, 2023, pp. 1–20.

[23] S. Deterding, D. Dixon, R. Khaled, and L. Nacke, “From Game Design Elements to Gamefulness: Defining Gamification,” in *Proceedings of MindTrek*, 2011, pp. 9–15.

[24] B. Alkhazi et al., “Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior,” *IEEE Access*, vol. 10, pp. 132319–132337, 2022.

[25] D. Emm, “Gamification - can it be applied to security awareness training?” *Network Security*, vol. 2021, no. 4, pp. 7–10, 2021.

[26] B. M. Bowen et al., “Measuring the Human Factor of Cyber Security,” in *IEEE Conference on Technologies for Homeland Security (HST)*, 2011, pp. 230–235.

[27] T. van Steen, M. Deeleman, and E. Norris, “What makes a cybersecurity awareness campaign successful? Investigating the efficacy of NIST-based measures via experience sampling,” *Computers & Security*, vol. 109, p. 102396, 2021.

[28] E. Amankwa, M. Loock, and E. Kritzinger, “Establishing Information Security Policy Compliance Culture in Organizations,” *Information & Computer Security*, vol. 26, no. 4, pp. 420–436, 2018.

[29] A. Birajdar and T. N. Nisha, “APPEARS Framework for evaluating Gamified Cyber Security Awareness Training,” in *2022 International Conference on Computing, Communication, and Intelligent Systems*, 2022, pp. 1–6.

[30] M. Hendrix, A. Al-Sherbaz, and V. Bloom, “Game Based Cyber Security Training: Are Serious Games Suitable for Cyber Security Training?” *International Journal of Serious Games*, vol. 3, no. 1, pp. 53–61, 2016.

[31] B. D. Cone, C. E. Irvine, M. F. Thompson, and T. D. Nguyen, “A Video Game for Cyber Security Training and Awareness,” *Computers & Security*, vol. 26, no. 1, pp. 63–72, 2007.

[32] I. Ghafir, V. Prenosil, A. Alhejailan, and M. Hammoudeh, “Social Engineering Attack Strategies and Defence Approaches,” in *IEEE International Conference on Social Computing and Networking*, 2016, pp. 145–149.

[33] R. Jouaibi, A. K. Gaylard, and B. A. Lee, “Employee Cyber-Security Awareness Training (CSAT) Programs in Ireland’s Financial Institutions,” in *2022 Cyber Research Conference - Ireland (Cyber-RCI)*, 2022, pp. 1–6.

[34] Supabase Inc., “Supabase Documentation: The Open Source Firebase Alternative,” 2025. [Online]. Available: https://supabase.com/docs.

[35] J. A. Bukhsh, M. Daneva, and M. van Sinderen, “Exploring User Risk Factors and Target Groups for Phishing Victimization in Pakistan,” *arXiv preprint arXiv:2510.09249*, 2025.

[36] K. Renaud, M. Volkamer, and A. Renkema-Padmos, “Why Doesn’t Jane Protect Her Privacy?” in *Proceedings of PETs Symposium*, vol. 2014, no. 4, pp. 244–262, 2014.

[37] Meta Open Source and React Team, “React: The Library for Web and Native User Interfaces,” 2025. [Online]. Available: https://react.dev/.

[38] E. You and Vite Team, “Vite: Next Generation Frontend Tooling,” 2025. [Online]. Available: https://vitejs.dev/guide/.

[39] A. Wathan and Tailwind Labs, “Tailwind CSS Documentation,” 2025. [Online]. Available: https://tailwindcss.com/docs.

[40] M. Hijji and G. Alam, “A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic,” *IEEE Access*, vol. 9, pp. 7152–7169, 2021.

[41] Y. Aydin, “Think First, Verify Always: Training Humans to Face AI Risks,” *arXiv preprint arXiv:2508.03714*, 2025.

[42] G. Canova, M. Volkamer, C. Bergmann, and R. Borza, “NoPhish: An Anti-Phishing Education App,” in *Security and Trust Management*, 2015, pp. 188–192.

[43] D. D. Caputo, S. L. Pfleeger, J. D. Freeman, and M. E. Johnson, “Going Spear Phishing: Exploring Embedded Training and Awareness,” *IEEE Security & Privacy*, vol. 12, no. 1, pp. 28–38, 2014.

[44] W. R. Flores and M. Ekstedt, “Shaping Intention to Resist Social Engineering through Transformational Leadership, Information Security Culture and Awareness,” *Computers & Security*, vol. 59, pp. 26–44, 2016.

[45] R. Wash, “Folk Models of Home Computer Security,” in *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, 2010, pp. 11:1–11:16.

[46] S. Furnell and N. Clarke, “Power to the People? The Evolving Recognition of Human Aspects of Security,” *Computers & Security*, vol. 31, no. 8, pp. 983–988, 2012.